IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Applicant: Challener	)	Art Unit: 2139
	)	
Serial No.: 10/748,919	)	Examiner: Young
	)	
Filed: December 22, 2003	)	RPS920030244US1
	)	
For: SYSTEM AND METHOD FOR CONTROLLING NETWORK ACCESS IN WIRELESS ENVIRONMENT	))))	November 3, 2007 750 B STREET, Suite 3120 San Diego, CA 92101

REPLY BRIEF

Commissioner of Patents and Trademarks

Dear Sir:

This responds to the Examiner's Answer dated October 10, 2007, apparently believing that if an apple is long enough and insistently enough declared to be an orange, persuasiveness has been achieved.

The apple: Sumner et al., paragraph 60 and relied on in the Answer, teaches that when a laptop roams to a new access point, it tries to log on, and if it is successful it is apparently given a full panoply of access. Otherwise, it doesn't, with absolutely no access as a consequence. There is no teaching of in-between access on the same network from the same access point in Sumner.

The first orange: a computer, if authorized, is given access to secure data on *the* network through *the* access point, and otherwise is given access to data other than the secure data on *the* network through *the* access point (Claim 1).

1191-4.RPL

CASE NO.: RPS920030244US1   PATENT
Serial No.: 10/748,919   Filed: December 22, 2003
November 3, 2007
Page 2

The second orange: if a predetermined communication hardware event has occurred, a computer is

selectively configured in a non-secure mode in which data on a network is accessed by the computer but not

all secure data available on the network can be accessed by the computer (Claim 7).

The third orange (similar to the first): a mobile computer is granted access to secure data on the

network through the access point if the access point is authorized for secure communication, and otherwise

the computer is granted access to data other than the secure data through the access point (Claim 14).

The fourth and final orange: based on a location or an identification of an access point, a computer

communicating with the access point is either granted access to secure assets in the network or is granted

access to other than the secure assets in the network (Claim 19).

Additionally, Appellant would like to point out that the conferees on the written record have admitted

that they are failing to apply the correct legal standard in construing the claims. Specifically, at the bottom

of page 10 the conferees admit that the standard they are using is a non-existent "broadest possible" standard

of claim interpretation, c.f. MPEP §2111.01 (claims to be given their broadest *reasonable* interpretation).

Since a non-existent legal standard of claim interpretation has on the written record been used in levying the

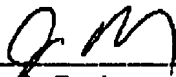rejections, reversal is clearly militated toward.

The response to Appellant's contentions regarding claims 6, 9, and 22 is so weak (simply declaring

that certain data would be "secure" without evidence and without tying the relied-upon data to other elements

are required by the claims) that Appellant will not belabor the Board's attention in further deconstruction.

1191-4.RPL

CASE NO.: RPS920030244US1   **PATENT**
Serial No.: 10/748,919   Filed: December 22, 2003
November 3, 2007
Page 3

Respectfully submitted,

John L. Rogitz
Registration No. 33,549
Attorney of Record
750 B Street, Suite 3120
San Diego, CA 92101
Telephone: (619) 338-8075

JLR:jg

1191-4.RPL.